COMPLIANCESUITE · 2026 EDITION

MiCA Readiness Checklist for CASPs

A 42-control self-assessment across the six MiCA domains. Source-cited against Regulation (EU) 2023/1114, the EU Travel Rule (Regulation 2023/1113), DORA and ESMA technical standards.

Domain	Controls	Primary references
1. Authorisation & Governance	8	MiCA Art. 59-68
2. AML / CFT & Travel Rule	9	AMLD6, Reg. 2023/1113
3. Onboarding & KYC	7	MiCA Art. 67-68
4. Custody & Safeguarding	6	MiCA Art. 75
5. Market Integrity & Conduct	6	MiCA Art. 88-92
6. Operational Resilience (DORA)	6	Reg. 2022/2554

How to use: walk each control with your MLRO. Mark Yes / Partial / No, attach the evidence reference, and assign an owner with a target date. Aim for 100% Yes before submitting your authorisation pack.

1. Authorisation & Governance

MiCA Articles 59-68

#	Control	Yes / Partial / No	Evidence ref.	Owner / due
1	Legal entity established in an EU Member State with a registered office and effective management.			
2	Programme of operations describing all CASP services (Art. 60).			
3	Governance arrangements: clear org chart, segregation of duties, three lines of defence.			
4	Suitability assessment for management body and qualifying shareholders (Art. 68).			
5	Prudential safeguards meeting Annex IV (own funds or insurance).			
6	Business continuity and ICT risk policy approved by the board.			
7	Conflicts of interest register, kept current and reviewed annually.			
8	Outsourcing policy with written agreements for all critical functions.			

2. AML / CFT & Travel Rule

AMLD6, Regulation 2023/1113

#	Control	Yes / Partial / No	Evidence ref.	Owner / due
1	Documented enterprise-wide ML/TF risk assessment refreshed at least annually.			
2	Customer risk-rating model with weighted factors (geo, product, channel, behaviour).			
3	Sanctions, PEP and adverse-media screening at onboarding and continuously thereafter.			
4	Transaction monitoring rule library mapped to FATF / EBA typologies.			
5	Travel Rule message exchange (IVMS-101) for transfers >= EUR 1 000 — including unhosted wallet handling.			
6	Suspicious-transaction reporting workflow producing goAML XML for the national FIU.			
7	Record-keeping: 5 years retention with tamper-evident storage.			
8	MLRO appointed, reporting line to the board, with an annual MLRO report.			
9	Independent AML audit performed at least every two years.			

3. Onboarding & KYC

MiCA Articles 67-68

#	Control	Yes / Partial / No	Evidence ref.	Owner / due
1	Identity verification using government-issued ID with NFC-chip read where available.			
2	Liveness detection at iBeta Level 2 or equivalent.			
3	Document forensics (MRZ, hologram, font and tamper checks).			
4	1:N biometric de-duplication to prevent multi-account abuse.			
5	Source-of-funds and source-of-wealth evidence for higher-risk segments.			
6	Periodic review cadence by risk band (e.g. low: 36m, medium: 18m, high: 6m).			
7	Re-verification triggered by behavioural or geographic anomalies.			

4. Custody & Safeguarding of Client Assets

MiCA Article 75

#	Control	Yes / Partial / No	Evidence ref.	Owner / due
1	Segregation of client crypto-assets from proprietary holdings on-chain.			
2	Custody policy covering key generation, storage, recovery and rotation.			
3	Daily reconciliation of on-chain balances against internal ledgers.			
4	Insurance or capital buffer for loss events; periodic stress test.			
5	Sub-custodian due diligence and ongoing monitoring.			
6	Client statements issued at least quarterly with audit trail.			

5. Market Integrity & Conduct

MiCA Articles 88-92

#	Control	Yes / Partial / No	Evidence ref.	Owner / due
1	Market abuse surveillance covering wash trading, spoofing and layering.			
2	Insider list maintained for all material non-public information events.			
3	STOR (suspicious transaction or order report) workflow to the supervisor.			
4	Pre- and post-trade transparency where applicable.			
5	Best-execution policy reviewed at least annually.			
6	Complaints-handling procedure with response SLA and regulator escalation path.			

6. Operational Resilience (DORA)

Regulation 2022/2554

#	Control	Yes / Partial / No	Evidence ref.	Owner / due
1	ICT risk management framework approved by the management body.			
2	ICT incident classification and reporting to the competent authority.			
3	Threat-led penetration testing for critical or important functions.			
4	Third-party ICT register with concentration-risk analysis.			
5	Business continuity plan with documented RTO and RPO per service.			
6	Annual digital operational resilience testing programme.			

Next steps

Run this checklist with your MLRO and ICT lead. Where you scored Partial or No, scope a remediation sprint with a named owner and a target date. ComplianceSuite automates 38 of the 42 controls out of the box — including Travel Rule messaging, STR / goAML generation, MiCA Article 80 incident reporting and the DORA ICT register.

Talk to our team

Book a 30-minute walk-through of how regulated CASPs operate this checklist live: compliancesuite.lovable.app/demo